ABSTRACT

An apparatus and method for random number generation, including a plurality of cross-connected latches 210, 215, 220, 225, providing at least two latch outputs (latch1, latch0) is provided. At least one input of one latch 210, 215, 220, 225 of the plurality of latches being driven by a clock signal 100. A first XOR 261 receives the at least two latch outputs (latch0, latch1) as an input, and generates a mistake signal "E" when its inputs do not match from the at least two latch outputs(latch0, latch1) being at different logic states. Te mistake signal is compared with a previously stored mistake signal by a second XOR 265 to determine whether to obtain a random bit from a pseudo random stream of bits.

Attorney Docket No.: US03 0063
Express Mail Label No.: EV 417136710 US